УДК 347.77(007:327.88)(477)

ІНФОРМАЦІЙНІ ВІЙНИ Й КІБЕРТЕРОРИЗМ: ПОНЯТТЯ, ОСОБЛИВОСТІ

Міщенко І.В., Басалюк Н.В., Таркін В.П.
Національний університет «Одеська юридична академія»

У статті викладено бачення інформаційних війн у різних наукових поглядах, у тому числі – авторських. На підставі аналізу літературних джерел, найбільш прийнятним видався підхід, що ґрунтується на виокремленні інформаційно-технічної та інформаційно-психологічної війн. У роботі було проведено паралель зазначених понять з дефініцією кібертероризм. З метою об'єктивного сприйняття інформаційних війн як процесу практичного виміру, наукове дослідження орієнтується та спрямовується, спираючись і на правовий аспект – у зв'язку з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» дане питання вивчалося з позицій вітчизняного законодавства.
Ключові слова: інформаційна війна, інформаційно-технічна війна, інформаційно-психологічна війна, інформаційна зброя, кібератака, кібертероризм.

Постановка проблеми. Актуальність теми зумовлена переходом інформації у розряд цінних ресурсів, який кличе до життя не лише бажання досягти мети – володіння ним, але й вбачає у ньому засіб – новий вид зброї, яка у певній мірі є не менш ефективним засобом впливу, ніж традиційне озброєння і військова техніка. Глобальна інформатизація зробила світове співтовариство, цілісність якого багато у чому забезпечується, у тому числі, за рахунок інтенсивного інформаційного обміну, більш вразливим – зупинка інформаційних контактів навіть на короткий час здатна призвести до кризи державного або навіть міжнародного рівнів. Сучасна науково-технічна революція породила нові форми конфліктів: інтенсивні, небезпечні, масштабні. Інформаційна цивілізація здійснила трансформацію поняття «агресія», яке набуло форм і особливостей «агресії інформаційної». У числі її складових – інформаційні війни й кібертероризм.

Аналіз останніх досліджень і публікацій. Вивченням питання інформаційних війн й кібертероризму займалися зарубіжні вчені: В. Голубєв у роботі «Кібертероризм – загроза національній безпеці», М. Лібікі «Що таке інформаційна війна?», В. Мазуров – «Кібертероризм: поняття, проблеми протидії», Е. Ріддайр, І. Панарін, Д. Фролов тощо. Вітчизняні науковці також розглядали зазначені явища у теоретичному й практичному аспектах, серед них – Г. Почепцов, В. Горбулін, Я. Жарков, М. Онищук, О. Саєнко, С. Степаниця та ін.

Виділення невирішених раніше частин загальної проблеми. Інформаційна ера впевнено крокує планетою, характеризується зростаючою роллю інформації в усіх сферах життя і діяльності людини, розглядає її як системоутворюючий фактор сучасного суспільства, що активно впливає на стан політичної, економічної, оборонної й інших складових безпеки держави. У цьому контексті актуальності набувають нові форми загроз – інформаційно-технічна й інформаційно-психологічна війна, кібертероризм, які проаналізовано як зі сторони теоретичних напрацювань, так і з позицій міжнародно-правового й вітчизняного правового регулювання, зокрема у контексті прийняття Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року.

Формування цілей. Під час написання роботи автори ставили перед собою наступні завдання: 1) здійснити аналіз літературних джерел із метою виявлення різних підходів до дефініції «інформаційна війна»; 2) викласти власне бачення щодо визначення інформаційних війн; 3) виявити особливості, ознаки інформаційних війн як гнучкої й прихованої форми впливу; 4) визначити стан розробленості проблеми у законодавстві; 5) проаналізувати співвідношення «кібертероризму» з дефініцією «інформаційні війни».

Викладення основного матеріалу. Інформаційна війна виникла як форма ескалації інформаційних конфліктів, це продукт розвитку суспільства, яке у XXI столітті стало свідком інформаційної революції.

У наукових роботах дефініція «інформаційна війна» має дискусійний характер. У рамках психологічної парадигми вона визначається як латентний вплив інформації на індивідуальну, групову, масову свідомість за допомогою методів пропаганди, дезінформації, маніпулювання з метою формування нових поглядів на соціально-політичну організацію суспільства через зміну ціннісних орієнтацій й базових установок особистості [7].

Сучасна наукова література виділяє й іншу точку зору, що базується на соціально-комунікативній концепції інформаційних війн. Згідно даного підходу у центрі предметного поля – не свідомість людей, а сама інформація. Так, М.А. Радіонов та В.С. Пірумов вбачають в інформаційній війні форму боротьби сторін, що складається із використанням спеціальних засобів і методів впливу на чужі інформаційні ресурси при захисті власного інформаційного капіталу [9].

Е.Б. Талишинський за допомогою різних підходів вивів поняття, що об'єднує вищеназвані підходи: інформаційна війна – це комплексний відкритий, чи закритий цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив сторін один на одного, що охоплює систему методів і засобів впливу на людей, їх психіку і поведінку, на інформаційні ресурси й інформаційні системи з метою досягнення інформаційної переваги у забезпеченні національної стратегії, здатної привести до прийняття необхідних для ініціатора впливу рішень чи паралізувати інформаційну структуру противника з одночасним захистом власної інформації й інформаційних систем [13].

У даній роботі застосуємо поліпарадигмальний підхід і виокремимо інформаційно-психоло-

гічну та інформаційно-технічну війни як окремі види, що можуть існувати незалежно один від одного. У цьому зв'язку під інформаційно-технічною війною розумітимемо будь-який тип інформаційного впливу із застосуванням інформаційної зброї, метою якого є порушення нормального функціонування інформаційної інфраструктури (дезорганізація роботи технічних засобів, долання системи захисту, обмеження доступу законних користувачів) з можливістю подальшого несанкціонованого збору, копіювання, блокування, видалення інформації. Синонімом даної дефініції може виступити «кібервійна». А під інформаційно-психологічною війною – наміри, зусилля, планові психологічні операції застосовані до певної аудиторії з метою впливу на їх свідомість, волю, емоції, мотиви, об'єктивні судження.

Особливостями інформаційно-технічної війни є складність ідентифікації джерела агресії, контрольоване, дозоване нанесення шкоди, припинення дії після повного досягнення цілей, непередбачуваність наслідків. Потенційно кібератака проти будь-якої держави може спровокувати масштабний уже міжнародний конфлікт, оскільки відповідь сторони, що постраждала, може бути непропорційною.

На міжнародному рівні, крім конвенційного регулювання у рамках Ради Європи основних засад співробітництва у протидії кіберзлочинності (Конвенція про кіберзлочинність від 23 листопада 2001 року), фактично зберігається правовий вакуум, пов'язаний з відсутністю спеціально розроблених норм і принципів, що регулюють конфлікти у кіберпросторі. Фахівці відмічають два варіанти вирішення цієї проблеми. Перший – піти шляхом вироблення загального підходу до застосування діючих норм міжнародного права, принципів гуманітарного права, що регулюватимуть застосування сили у кіберпросторі. Однак кіберпростору в цілому, й інформації, зокрема, властиві ряд унікальних просторово-часових характеристик, подільність і відтворюваність, що викличе необхідність подальшого опрацювання ключових понять «війна», «зброя», «агресія», «застосування сили» у контексті кібербезпеки. Другий – розробка й прийняття нового комплексного, юридично обов'язкового документу, який би регулював всі аспекти використання інформаційно-комунікаційних технологій у цілях, що суперечать завданню забезпечення міжнародного миру і стабільності [1].

Щодо рівня національного, то 5 жовтня 2017 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон). Навіть поверхневий огляд дає можливість виявити його надмірну теоретичну спрямованість і перенасичення нормами-принципами. Так, стаття 2 «Принципи застосування Закону» у першій частині містить винятки зі сфери дії цього законодавчого акту, у другій – власне принципи. Викликає подив такий підхід законодавця, адже, принципи прозорості, недискримінації, забезпечення захисту в тому числі прав щодо невтручання у приватне життя і захисту персональних даних тощо вже передбачені Конституцією України та іншими законами України, їх наявність ніяк не полегшить застосування витіюватих положень цього Закону. Стаття 7 аналізованого Закону містить іще один перелік принципів – на цей раз забезпечення кібербезпеки. Законодавець і тут не пішов шляхом «винаходу велосипеда» і помістив у статтю всім відомі принципи верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту у порядку, визначеному законом, невідворотності покарання за вчинення кіберзлочинів, міжнародного співробітництва і т.д.

Некритичне запозичення юридичної термінології, а інколи й цілих інститутів – тенденція у нашій країні непоодинока, але якщо велика кількість з них «прищеплюється» українському законодавству із західної доктрини і практики, то пропоновані дефініції у новому законі є далеко не новелами. Стаття 1 цього Закону являє собою зібрання звичних «злочин», «оборона», «шпигунство», «тероризм» тощо із префіксом «кібер-». Не всі поняття є узгодженими: до прикладу, кібербезпека і безпека електронних інформаційних ресурсів, кіберзлочин й комп'ютерна надзвичайна подія. На особливу увагу заслуговує неодноразово згадуваний «кіберпростір», визначення поняття якого в законі саме вимагає пояснення, адже на головне питання «які його межі?» відповіді немає. Зрозуміло, що кіберпростір через свою віртуальну природу не може мати якихось чітких меж. Однак включення цього терміну до понятійно-категоріального апарату аналізованого Закону, наділення низки державних органів повноваженнями у кіберпросторі передбачає необхідність його втілення на практиці. Зважаючи на те, що у Прикінцевих положеннях не йдеться про внесення змін до Закону України «Про державний кордон» від 4 листопада 1991 року з метою їх встановлення, очевидно, що законодавець межі кіберпростору, на який має поширюватися юрисдикція українських державних інституцій, не прив'язує до державного кордону та державної території. У цьому зв'язку виникає логічне питання: яким чином, приміром, Служба безпеки України здійснюватиме запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, як буде розмежовуватися її компетенція та аналогічних органів іноземних держав? Отже, виникає побоювання, що зазначена категорія так і залишиться абстрактною юридичною конструкцією, позбавленою практичної реалізації.

Під критично важливими об'єктами інфраструктури у статті 1 розуміються підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [10]. Словосполучення «незалежно від форм власності» при визначенні поняття вказує, що до об'єктів належатимуть, у тому числі приватні компанії, причому задіяні не лише у сфері інформаційних технологій, елек-

тронних комунікацій, наданні послуг зв'язку, але й у галузях сільського господарства, хімічної промисловості, транспорту тощо. Недоліком визначення поняття є його оціночні судження: «велике значення», «негативний вплив». Не уточнення підстав дозволяє віднести до цієї категорії велику кількість підприємств. Такі нововведення обернуться для приватного сектору економіки, різних бізнес структур сфери інформаційних технологій значними фінансовими витратами, хвилею перевірок.

Не надто зрозумілим, виходячи з положень нового Закону, видається співвідношення категорій «кібербезпека» та «національна безпека». Логічно припустити, що вони співвідносяться як частина і ціле. На користь такого розуміння виступає віднесення законодавцем до правових основ забезпечення кібербезпеки України, серед іншого, законів України щодо основ національної безпеки, а так само пряме посилання на Закон України «Про основи національної безпеки України» від 19 червня 2003 року у частині визначення окремих термінів. Однак, якщо проаналізувати об'єкти національної безпеки та кібербезпеки, знаходимо певні протиріччя. Так, досить спірним є визначення в якості об'єкта кібербезпеки національних інтересів в усіх сферах життєдіяльності особи, суспільства та держави, а так само об'єкти критичної інфраструктури. Подібне формулювання не узгоджується з положеннями вищезгаданого Закону України «Про основи національної безпеки України», який об'єктами національної безпеки називає: людину і громадянина – їхні конституційні права і свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; державу – її конституційний лад, суверенітет, територіальну цілісність і недоторканність [11]. Крім того, розглядати національні інтереси в якості об'єкта кібербезпеки, як і національної безпеки взагалі, некоректно, зважаючи на те, що безпека – одна з базових потреб людини. Тому національну безпеку доцільніше розглядати як частину національних інтересів. Недоречно, на наш погляд, ставити в один ряд об'єктів кібербезпеки поряд з конституційними правами, суспільством, територіальною цілісністю держави тощо об'єкти критичної інфраструктури, тобто окремі підприємства, якими б важливими вони не були. Це явно різнорівневі категорії, яким, очевидно, не місце в одній статті Закону. Таким чином, вважаємо за доцільне вилучити з ч. 1 статті 4 «Об'єкти кібербезпеки та кіберзахисту» Закону України «Про основні засади забезпечення кібербезпеки України» пункт 4, який містить слова «національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави», та пункт 5 – «об'єкти критичної інфраструктури».

До основних суб'єктів забезпечення кібербезпеки належить 7 органів: Державна служба спеціального зв'язку та захисту інформації, Національна поліція, Національний банк України, Міністерство оборони, Генеральний штаб Збройних Сил, Служба безпеки України, розвідувальні органи. Неможливість зосередження управління кіберпростором «в одних руках», у силу специфіки об'єкта регулювання зумовило «розпорошення» повноважень. Головне, щоб це не відобразило старе-добре: «У сімох няньок дитина без нагляду», адже окремі повноваження без їх практичного впровадження уже викликають побоювання. Так, Служба безпеки України «негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів». Чи означатиме це, що СБУ на цілком законних підставах матиме змогу порушувати нормальне функціонування внутрішніх інформаційних систем підприємств, отримувати доступ до їх інформації, можливо навіть зі статусом «службова», «конфіденційна»? Зважаючи на міцно утверджені корупційні зв'язки таке розширення повноважень може призвести до зловживань, у вигляді, наприклад, знищення конкурентів. У ч. 3 ст. 15 містяться положення щодо необхідності подання щорічних звітів про результати проведення незалежного аудиту сімох названих суб'єктів, з огляду на правовий статус яких не є зрозумілим, до компетенції якого органу (чи суб'єкта) буде входити обов'язок проведення незалежного аудиту їх діяльності.

До завдань Державної служби спеціального зв'язку та захисту інформації віднесено й забезпечення функціонування Державного центру кіберзахисту та урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (Computer Emergency Response Team of Ukraine). Правовий статус Державного центру кіберзахисту не розкриває ані Закон України «Про державну службу спеціального зв'язку та захисту інформації», ані новий закон, ані будь-який чинний на сьогодні нормативно-правовий акт, але центр – не юридична фікція, а реально існуючий із 1 липня 2015 року при Державній службі. У цьому аспекті не зовсім зрозуміло, по-перше, до чого саме зводиться зобов'язання Державної служби «забезпечити функціонування» – матеріальне, технічне – яке? По-друге, який статус матиме CERT-UA та Державний центр кіберзахисту, адже, CERT-UA – спеціалізований структурний підрозділ Державного центру кіберзахисту – зайве наголошувати у законі ще й на ньому, як на окремому органі. У якому він статусі – фактично існуючому, спеціальному?.. За попередньою інформацією в Україні планується створення Центру кібербезпеки за стандартами НАТО. Але, коли плани фактично втілюватимуться – невідомо, як і статус існуючого Державного центру кіберзахисту у контексті закону.

Попри названі недоліки, у цілому, прийняття закону про кібербезпеку надзвичайно актуальне. Підтвердженням тому є події весни 2017 року, коли Європа опинилася «у полоні» вірусу Petya-A, який 27 червня підібрався й до України. Вірусом були вражені комп'ютерні системи «Укренерго», «Київенерго», «Епіцентр», «Київстар», Vodafone, Lifecell, канал ATR, аеропорт «Бориспіль», мережа автозаправочних станцій WOG, «Укргазвидобування» та інших. «Під удар» потрапив навіть сайт Кіберполіції України. Війна поступово втрачає свою матеріальну природу: hightech-технології будують hightech-світ – питання захисту власної інформаційної системи, вироблення стратегії роботи із інформаційною зброєю таке ж важливе як високоточні

ракети, кораблі й військові літаки в оборонному арсеналі країни. І хоча у законі прямо не визначено поняття «кібервійна» чи «інформаційна війна», надається визначення такому поняттю як «кібератака». Якщо вважати, що інформаційно-технічну війну характеризує застосування декількох кібератак, то можна сказати, що законодавець все ж підібрався до визначення цього широкого поняття.

Серед форм інформаційних атак виділяють: 1) активну атаку, у результаті якої фактично змінюються чи знищуються збережені, оброблені дані чи інші елементи ресурсу; 2) асинхронну атаку, при якій використовуються переваги динамічної дії системи, що дає змогу керувати вибором часу виконання тих чи інших дій; 3) контрольовану атаку, що направлена на основний потік повідомлень у мережі Ethernet (протокол кабельних комп'ютерних мереж) і подальшу зміну рухів для повідомлень певного виду із з певними ознаками (наприклад такими, що містять конкретні паролі); 4) пасивну атаку, при якій знімається обмеження на доступ до даних чи змінюється форма контролю за доступом до них [6].

У арсеналі інформаційної зброї театру військових дій комп'ютерні віруси, логічні бомби (команди, заздалегідь вбудовані у програму, що спрацьовують у потрібний момент), фальсифікація інформації, засоби нейтралізації тестових програм й різного роду помилки, що свідомо вводяться у програмне забезпечення [12].

Цілеспрямований вплив на психіку, масову та індивідуальну свідомість людей для зміни або використання їхнього світогляду, цінностей, моральних переконань, щоб послабити або нівелювати психологічний опір відносно певних моделей поведінки характеризує інший вид – інформаційно-психологічну війну. Цей негативний суспільний прояв, що посягає на один з об'єктів національної безпеки – духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне середовище отримав назву інформаційно-психологічної війни. Легальної дефініції поняття інформаційно-психологічна війна законодавець не надає, однак, у статті 7 Закону України «Про основи національної безпеки» серед загроз національним інтересам й національній безпеці в інформаційній сфері говориться про намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Парфенюк І. розрізняє два види інформаційно-психологічної війни: стандартну інформаційну війну – це інформаційна війна, у якій під час цілеспрямованого інформаційного впливу активно задіяний інформаційний простір, а також культурні цінності, ціннісні орієнтації, символи, світогляд та інші компоненти культурного простору, в якому знаходиться об'єкт впливу й стратегічну інформаційну війну – це інформаційна війна, під час якої здійснюється вплив на інформаційний та культурний простір об'єкта з метою їх трансформації, що призведе до змін у культурних цінностях, світобаченні та поведінці об'єкта інформаційної агресії [8].

Інформаційно-психологічна війна характеризується цілим рядом прийомів, першим з яких можна визнати пропаганду. Як зазначає Е. Бернейс, у широкому сенсі, пропаганда – організована діяльність із розповсюдження того чи іншого переконання чи доктрини, механізм широкомасштабного навіювання поглядів [2]. Епоха всезагальної грамотності дала людині набір штампів, реклами, «наукових» даних і спотворену історію, натомість – відібрала оригінальність думки і незалежність помислів. Маси піддаються формування думок, який задає вектор їх свіжих сил на суворо визначені цілі.

До форм пропаганди можна віднести: 1) приклеювання або навішування так званих «ярликів», для позначення, іменування людини, організації, ідеї, будь-якого соціального явища. Ці «ярлики» викликають емоційно негативне ставлення, асоціюються з ганебними вчинками і, таким чином, використовуються для того, щоб зганьбити особистість або соціальну групу; 2) посилання на авторитет – зміст цього прийому полягає у наведенні висловлювань особистостей, які користуються великим авторитетом або ж навпаки, таких, які викликають негативну реакцію у категорії людей, на яких спрямовується маніпулятивний вплив. Мета полягає у встановленні довірливих стосунків з аудиторією. Такими групами впливу можуть бути відомі політичні діячі, діячі культури, відомі актори; 3) «загальний вагон» – при використанні цього прийому здійснюється підбір суджень, висловлювань, фраз, які вимагають одноманітності в поведінці, що створюють враження, ніби так роблять усі; 4) «зворотний ефект» – відбувається викид такої кількості негативної інформації на адресу якоїсь особи, що ця інформація досягає прямо протилежного ефекту, і замість засудження вона починає викликає жалість; 5) правда наполовину – публіці подається лише частина достовірної інформації; 6) захоплення медіапростору – прийом полягає в тому, що пропагандист працює зі всілякими ЗМІ і при цьому не дає діяти в інформаційному полі іншим організаціям. Таким чином, споживач отримує інформацію тільки від цієї організації і вважає її єдино правильною [2]; 7) висміювання, якому можуть бути піддані як конкретні особи, так і погляди, ідеї, програми, організації та їх діяльність, різні об'єднання людей, проти яких ведеться боротьба; 8) провокації як технології інформаційної війни – якщо події відсутні або їм не вистачає резонансу, їх завжди можна вигадати.

До інших прийомів інформаційно-психологічного впливу можна віднести: дезінформування та маніпулювання, диверсифікація громадської думки, психологічний тиск, поширення чуток [5].

Інформаційні війни не слід ототожнювати із інформаційним терористичним актом. Легальне визначення поняття «кібертероризму» міститься у прийнятому 5 жовтня 2017 року Законі України «Про основні засади забезпечення кібербезпеки України», де під ним розуміється терористична діяльність, що здійснюється у кіберпросторі або з його використанням. Чи можна таку конструкцію уважати у майбутньому робочим правовим механізмом – швидше ні, оскільки наведене поняття містить у собі «замкнене коло»: кібертероризм – терористична діяльність, являє ще одну громіздку конструкцію, яка навряд чи знайде

своє практичне втілення, оскільки і матеріальне кримінальне, і процесуальне кримінальне право й надалі оперуватимуть звичним «тероризмом».

Свої підходи до завдання виокремити сутнісні ознаки даного явища виробила й юридична доктрина. В.А. Голубєв під кібертероризмом розуміє умисну атаку на інформацію, комп'ютерну систему чи мережу, яка створює небезпеку для життя і здоров'я людей чи може призвести до настання інших тяжких наслідків, якщо такі дії були скоєні із метою порушення суспільної безпеки, залякування населення чи провокацією воєнного конфлікту [4]. Васенін В.А. визначає комп'ютерний тероризм як сукупність протиправних дій, пов'язаних із замахом на життя людей, погрозами розправ, деструктивними діями у відношенні матеріальних об'єктів, спотворення об'єктивної інформації чи рядом інших дій, що сприяють поширенню страху й напруги у суспільстві із метою отримання переваг при вирішенні політичних, економічних чи соціальних проблем шляхом руйнування інформаційної інфраструктури, виведення із ладу системи управління нею чи несанкціонованого доступу до мережевої інформації, порушення її цілісності, конструктивного керування й захищеності [3]. З такими визначеннями можна погодитися, адже у них автори зосереджують увагу на двох визначальних для кібертероризму аспектах – меті, яка залишається тотожна звичайному терористичному акту із наближенням до законодавчого визначення терористичного акту, викладеного у ст. 258 Кримінального кодексу України й інформаційному середовищі.

Засоби здійснення інформаційно-терористичних дій можуть варіюватися у широких межах і включати усі вище перелічені види інформаційної зброї. У той же час тактика й прийоми інформаційного терору суттєво відрізняються від тактики інформаційно-технічної війни й прийомів інформаційного криміналу. Для кібертерориста головне, щоб дії мали небезпечні наслідки, стали широко відомими населенню й отримали суспільний резонанс.

Як й інформаційно-технічна війна, кібертеракт не має державних меж, кібертерорист може рівною мірою створити загрозу інформаційним системам, розташованим у будь-якій точці земної кулі. Виявити й нейтралізувати віртуального терориста практично неможливо через малу кількість залишених ним слідів. На відміну від звичайного терориста, який для досягнення своєї мети використовує вибухівку, у руках кібертерориста – сучасні інформаційні технології та необхідний рівень технічної підготовки для запуску кібербомби. Причому, кібертерористом може бути як учасник терористичної групи, так і окрема особа, що розділяє її погляди (релігійні, політичні тощо).

Порівнюючи інформаційно-психологічну війну й кібертероризм, варто сказати, що одним із способів кібертероризму є «атака на інформацію». Якщо звичайна інформаційна війна ведеться з метою впливу, маніпуляції, кібертероризм відрізняється вужчою спрямованістю і ставить перед собою завдання залякування: погроза насилля, підтримання стану страху з метою досягнення політичних цілей, пропагування поглядів, виклик культурі й цивілізації.

Висновки. Сьогодні у боротьбі за сфери економічного й політичного впливу акцент із застосування фізичної сили усе більше зміщується на сторону прихованих й гнучких форм агресії, у числі яких – інформаційні війни й кібертероризм. Теоретичний аналіз даних понять дозволяє виявити, що інформаційна війна – складний, багатофакторний об'єкт, а велика кількість аргументованих концепцій обумовлена тим, що автори належать до різних наукових шкіл та диференційовано підходять до методологічних засад визначення області дослідження. Від інформаційних війн слід відрізняти кібертероризм, що має чітко визначену ціль наближену до тієї, що ми вкладаємо у традиційне уявлення про терористичний акт. Епоха інформаційного суспільства, що поставила собі на службу телекомунікації й глобальні мережі ще не одного разу здивується які можливості для зловживань створюють ці технології, питання захисту від кібернападів знову і знову ставатиме предметом дискусії серед публіцистів, науковців, техніків, законодавців.

Перший законодавчий механізм забезпечення можливості подолання, а в ідеалі – недопущення зазначених вище негативних явищ однозначно заслуговує схвалення, навіть незважаючи на наявні суттєві недоліки. Їх усунення, а так само розробка належної підзаконної бази, сподіваємось, надасть можливість у майбутньому чинити гідний опір викликам і загрозам, що спіткають нашу державу протягом останніх років.

Список літератури:

1. Батуева Е. Информационная война США: к определению национальной киберстратегии / Е. Батуева // – [Електронний ресурс]. – Режим доступу: http://www.intertrends.ru/thirty-seventh/Batueva.pdf – Назва з екрану.
2. Бернейс Э. Пропаганда / Э. Бернейс // И-во: Карьера-Пресс. – 2015. – 176 с.
3. Васенин В.А. Информационная безопасность и компьютерный терроризм [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/articles/vasenin – Назва з екрану.
4. Голубев В.А. Кибертерроризм – узроза национальной безопасности [Электронный ресурс]. – Режим доступа: http://www.crimeresearch.ru/articles/Golubev_Cyber_Terrorism/2 – Назва з екрану.
5. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення / Ю.О. Горбань // Вісник НАДУ. – 2015. – № 1. – С. 136–141.
6. Информационная война и защита информации. Словарь основных терминов и опередедений. – Москва. – 2011. – 68 с.
7. Кунакова Л.Н. Информационная война как объект научного анализа (понятие и основне характеристики информационной войны) / Л.Н. Кунакова // Альманах современной науки и образования. – Тамбов: Грамота. – 2012. – № 6(61). – С. 93–96.
8. Парфенюк І. Стратегічні та стандартні інформаційні війни в Україні (на прикладі інформаційної агресії РФ) / І. Парфенюк // Український інформаційний простір. Число 2. – 2014. – С. 298–305.

9. Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5. С. 44–47.
10. Про основні засади забезпечення кібербезпеки України: проект закону від 19 червня 2015 р. № 2126а. – 2015. – [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657 – Назва з екрану.
11. Про основи національної безпеки: Закон України від 19 червня 2003 р. № 964-IV / Голос України // 2003. – № 134.
12. Расторгуев С.П. Информационная война / С.П. Расторгуев // М.: Радио и свіязь. – 1999. – 222 с.
13. Талышинский Э.Б. Сущность информационной войны в процессах глобализации / Э.Б. Талышинский // Університетські наукові записки. – 2012. – № 2(42). – С. 385–389.

Мищенко И.В., Басалюк Н.В., Таркин В.П.
Национальный университет «Одесская юридическая академия»

ИНФОРМАЦИОННЫЕ ВОЙНЫ И КИБЕРТЕРОРРИЗМ: ПОНЯТИЕ, ОСОБЕННОСТИ

Аннотация
В статье изложено видение информационных войн в различных научных взглядах, в том числе – авторских. На основании анализа литературных источников, наиболее приемлемым оказался подход, основанный на выделении информационно-технической и информационно-психологической войн. В работе проведена параллель указанных понятий с дефиницией кибертерроризм. С целью объективного восприятия информационных войн как процесса практического измерения, научное исследование ориентируется и направляется, опираясь и на правовой аспект: в связи с принятием Закона Украины «Об основных принципах обеспечения кибербезопасности Украины» данный вопрос изучался с позиций отечественного законодательства.
Ключевые слова: информационная война, информационно-техническая война, информационно-психологическая война, информационная оружие, кибератака, кибертерроризм.

Mischenko I.V., Basalyuk N.V., Tarkin V.P.
National University «Odessa Academy of Law»

THE NOTION AND FEATURES OF INFORMATION WARS AND CYBERTERRORISM

Summary
The article outlines the vision of information wars in various scientific views, including the author's one. Under the analysis of literary sources, the most acceptable was the approach based on the differentiation of information technology warfare and psychological warfare; was drawn a parallel between the above concepts and the definition of cyberterrorism. Research article is relying on the legal aspect for impersonal assessment of information wars as a process of practical measurement. In connection with the passing of the Law of Ukraine «On the basic principles of the protection of cybersecurity of Ukraine» this issue was also studied from the standpoint of national legislation.
Keywords: information war, information technology warfare, psychological warfare, information weapons, cyberattack, cyberterrorism.